PRIVACY POLICY STATEMENT

1 Statement

The Sport for All Confederation of Hong Kong, China Limited (the Confederation), as a Data User, respects personal data privacy and is committed to fully implementing and complying with the data protection principles and all relevant provisions of the Personal Data (Privacy) Ordinance (Cap 486) and codes of practice issued by the Privacy Commissioner for Personal Data. The Confederation is equally committed to ensuring that all its officials, staff and agents uphold these obligations. The Confederation undertakes to:

1.1 collect personal data directly related to the functions and activities of the Federation only for lawful purposes, and by lawful and fair means;

1.2 take all reasonably practicable steps to ensure that personal data are accurate, up-to-date and kept no longer than necessary;

1.3 use the personal data collected only for purposes or directly related purposes for which the data were to be used at the time of collection, unless the Data Subject concerned has given his consent to a change of use or such use is permitted by law;

1.4 take all reasonably practicable steps to ensure that personal data are protected against unauthorized or accidental access, processing, erasure or other use;

1.5 take all reasonably practicable steps to ensure that the public is informed of the kinds of personal data that the Federation holds and the purposes for which the data are to be used; and

1.6 permit Data Subjects to access and correct their personal data and process the data access / correction requests in a manner permitted or required by law.

2 Types of Personal Data Processed by the Federation

The Confederation, in the course of its operations, may process the following types of personal data of Officers, Committee Members, members, athletes, staff, participants and other individuals:

2.1 Identification data (e.g. name and Hong Kong Identity Card / passport details);

2.2 Personal details (e.g. age, sex, date of birth, marital status, occupation, address, telephone number, e-mail address and other contact details);

2.3 Employment record (e.g. job applications, past and present staff's job particulars, details of salary, payments, benefits, leave, training records, group medical and dental insurance records, mandatory provident fund schemes participation, performance appraisals, and disciplinary matters);

2.4 Payment details (e.g. bank / credit card details, for enrolment of events / activities);

2.5 Health information (e.g. data from medical / anti-doping tests and emergency contact details);

2.6 Vehicle information (e.g. car plate number, for the use of parking facilities at the Olympic House or at venues of events / activities); and

2.7 Images (e.g. photo of an individual participating in the Federation's events / activities, and image of a visitor to the Olympic House captured by CCTV system).

3 Main Purposes for Processing Personal Data

3.1 The purposes for which the Federation processes personal data are:

3.1.1 To verify an individual's identity;

3.1.2 To ensure compliance with the rules and regulations of the Federation and that of international sports governing bodies;

3.1.3 To maintain and develop services, including programmes, activities, and events;

3.1.4 To enable athletes and officials to participate in international multi-sports Games, including the selection of potential athletes into the Hong Kong, China Delegation;

3.1.5 To organize, conduct and promote the Federation's events / activities;

3.1.6 To maintain relationships with the Federation's members;

3.1.7 To handle complaints / enquiries as appropriate;

3.1.8 To carry out surveys and statistical analyses;

3.1.9 For purposes related to recruitment of staff, manpower management, and maintenance of employment relationship;

3.1.10 For security purposes; and

3.1.11 Where otherwise reasonably necessary for the Confederation to carry out its functions.

4 Lawful Bases for Processing Personal Data

4.1 The Confederation only processes personal data where there is a lawful basis for doing so.

4.1.1 Consent: the Data Subject has given clear consent for the Confederation to process their personal data for a specific purpose.

4.1.2 Contract: the processing is necessary for a contract the Confederation has with a Data Subject, or because a Data Subject has asked the Confederation to take specific steps before entering into a contract.

4.1.3 Legal obligation: the processing is necessary for the Confederation to comply with the law.

4.1.4 Vital interests: the processing is necessary to protect the Data Subject's life.

4.1.5 Public task: the processing is necessary for the Confederation to perform a task in the public interest.

4.1.6 Legitimate interests: the processing is necessary for the Confederation's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

4.2 In addition, the Confederation will on occasion need to process special category personal data (e.g. when conducting medical / anti-doping tests) or criminal records information (e.g. when carrying out No Criminal / Sexual Conviction Record Checks) in accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required.

5 How the Confederation Collects Personal Data

5.1 Generally, the Federation collects personal data from the individual directly. This may be via a form, an online platform or simply in the ordinary course of interaction or communication.

5.2 In some cases, personal data will be supplied by third parties (e.g. a National Sports Association or other professionals or authorities working with that individual) or collected from publicly available resources.

5.3 The Confederation will not collect personal data from a minor without prior consent from a person with parental responsibility for the minor.

6 Access to and Sharing of Personal Data

6.1 The Confederation may be required to share personal data with third parties, such as:

6.1.1 professional advisers (e.g. lawyers, insurers and auditors);

6.1.2 government authorities;

6.1.3 partners or related organizations (e.g. International Olympic Committee, Organizing Committee of multi-sports Games); and

6.1.4 where appropriate, parties who will be contacted by us during the handling of a complaint / enquiry case including the party being complained against and/or other parties concerned.

6.2 For the most part, personal data collected by the Confederation will remain within the Confederation and will be processed by appropriate individuals on a “need to know” basis.

6.3 Some of the Confederation’s processing activity is carried out on its behalf by third parties, such as IT systems, web developers or cloud storage providers. All the Federation’s service providers are bound by contractual duty to keep confidential any data they come into contact with against unauthorized access, use and retention.

7 Information Collected on the Confederation’s Websites

7.1 A cookie is a small amount of data created in a computer when a person visits a website on the computer. It often includes an anonymous unique identifier. A cookie can be used to identify a computer. Cookies are used by the Confederation to collect statistics about the number of visits of users to the Confederation’s websites and the users' preference of websites and online services offered on the Confederation’s websites. Users may choose to accept or reject cookies. If users reject cookies, they will not be able to use some of the functions of the websites, such as saving preferences and accessing some online services.

7.2 When a user visits the Confederation's websites, the webserver makes a record of the visit that includes the user's IP addresses (and domain names), the types and configurations of browsers, language settings, geo-locations, operating systems, previous sites visited, and time/duration and the pages visited (webserver access log). The Confederation uses the webserver access log for the purpose of maintaining and improving its websites such as to determine the optimal screen resolution, which pages have been most frequently visited etc. The Confederation uses such data only for website enhancement and optimization purposes. The Confederation does not use, and have no intention of using the visitor data to personally identify anyone.

8 Protection Measures

The Confederation takes appropriate steps to protect the personal data it holds against loss, unauthorized access, use, modification or disclosure. For example, training on personal data protection is provided to staff members who need to handle personal data in their daily work.

9 Retention

Personal data will not be kept longer than is necessary for the fulfilment of the purpose for which it is collected. Personal data that is no longer needed is either irreversibly anonymized (and the anonymized information will be retained) or securely destroyed.

10 Data Access and Correction

10.1 Data access requests should be made in writing using the form prescribed by the Privacy Commissioner for Personal Data[1]. The completed form should be sent directly to the Data Protection Officer by fax (2891 3657), by email (secretariat@sportforallhk.org), or in person or by post to:

Sport for All Confederation of Hong Kong, China Limited
1032A, Olympic House
1 Stadium Path, Causeway Bay,
So Kon Po, Hong Kong

10.2 When handling a data access or correction request, the Confederation will check the identity of the requester to ensure that he is the person legally entitled to make the data access or correction request.

11 Enquiries

Any enquiries regarding the Federation's personal data privacy policy and practice may be addressed to the Data Protection Officer by post to the above correspondence address, via email to secretariat@sportforallhk.org or by telephone to 2504 8642 during office hours.

The Confederation's Privacy Policy Statement is kept under regular review. This statement was last updated on 8 May 2019.

[1] The data access request form is available on the Office of the Privacy Commissioner for Personal Data's website: https://www.pcpd.org.hk/english/publications/files/Dforme.pdf.

CODE OF PRACTICE ON DATA PROTECTION

1 Introduction

This Code of Practice provides guidance and good practices in safeguarding personal data privacy and ensures the Confederation's compliance with the Personal Data (Privacy) Ordinance (Cap. 486). The Confederation shall ensure that it is made known to all Officials of the Confederation, including Officers, Committee Members and staff members. Sections marked with asterisks (*****) are particularly relevant to all staff members.

2 Definition of Personal Data*

Personal data refers to information that relates to a living person and can be used to identify that person. It exists in a form in which access to or processing of is practicable. Examples of personal data protected by the Ordinance include names, phone numbers, addresses, identity card numbers, photos, medical records and employment records, etc.

3 Six Data Protection Principles

3.1 The Privacy Commissioner for Personal Data recognizes six Data Protection Principles (DPPs) that represent the core of the Ordinance:

- DPP1 - Data Collection Principle
- DPP2 - Accuracy & Retention Principle
- DPP3 - Data Use Principle
- DPP4 - Data Security Principle
- DPP5 - Openness Principle
- DPP6 - Data Access & Correction Principle

3.2 The following paragraphs provide practical guidance on how to adhere to the six DPPs:-

4 Collection of Personal Data (DPP1)*

4.1 The purpose of collection must be directly related to the functions or activities of the Confederation, and the data collected in relation to a specified purpose should be adequate but not excessive.

4.2 During the collection of personal data, Data Subjects should be informed explicitly of the following:

4.2.1 purpose for which the data is collected;

4.2.2 parties to whom the data may be transferred;

4.2.3 whether it is obligatory or voluntary to supply the data, and the consequences of not doing so;

4.2.4 rights of the Data Subject to request access to and correction of the data held by the Confederation; and

4.2.5 the person to be contacted for data access and correction.

4.3 A Personal Information Collection Statement (PICS) should be included when collecting personal data directly from a Data Subject. **Appendix I** lists out some circumstances under which a PICS is or is not required. A sample of PICS is shown at **Appendix II**.

4.4 When proposing to collect HKID card numbers or copies, consideration should be given to adopting other less privacy-intrusive alternatives. For example, collecting the first four digits of HKID card numbers should be sufficient for the purpose of identification of persons with the same names. Staff cards or other photo identification documents could be used instead of HKID card to check the identity of a person. For further information, reference should be made to the relevant Code of Practice[2] issued by the Office of the Privacy Commissioner for Personal Data.

5 Accuracy and Retention of Personal Data (DPP2)*

5.1 Officials holding personal data should review and update the personal data they keep periodically to ensure that it is accurate. Inaccurate data and data no longer in use should be deleted.

5.2 The Federation should keep a personal data inventory to keep track of the types of personal data it holds and how the personal data is being processed. Each Office Head should prepare the updated personal data inventory of his/her respective office annually (or when there is any new project that involves the collection of a new category of personal data) and submit it to the Data Protection Officer (DPO) for filing. A sample personal data inventory is shown at **Appendix III**.

5.3 Officials should ensure that personal data is not kept longer than necessary to fulfil the purpose for which it is used.

5.4 As a good practice, personal data not collected directly by the Confederation but transferred from another source should be disposed of properly immediately after use. Fresh data should be requested each time it is required.

5.5 The below table shows the recommended maximum retention periods for different types of personal data held by the Federation:

Type of Personal Data		**Maximum Retention Period**
Secretariat		
Events / Programmes	Personal data of past participants	7 years from the completion of the event / programme
Multi-sports Games	Personal data of Delegation members	8 years from the completion of the Games in accordance with the Financial Guidelines of Olympic Solidarity

[2] https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/com,pliance_guide_e.pdf

Type of Personal Data		Maximum Retention Period
Membership	Personal data of past individual members / representatives of member associations	2 years from the date of cessation of membership / representation
Employment Record	Job applications of unsuccessful candidates	2 years from the completion of the recruitment exercise
	Personal files of past employees	7 years from the date of cessation of employment
Complaints	Personal data of complainants / complainees	2 years from the completion of the complaint, after which all related personal data shall be deleted or anonymized (unless there is any relevant statutory or regulatory requirements to keep the data for a longer period of time)
Education Programmes	Personal data of past speakers	7 years from the completion of the seminar / talk / event
Exchange Programmes	Personal data of Delegation members	7 years from the completion of the programme
Study Tours	Personal data of participants	7 years from the completion of the session / course / tour
Competitions & Fundraising Events	Personal data of participants	7 years from the completion of the competition / fundraising event

5.6 In direct marketing (e.g. promoting programmes / activities, soliciting donations / contributions, etc.):

5.6.1 Written or verbal consent must be obtained from Data Subjects for the use of their personal data. Data Subjects should also be informed of the classes of marketing subjects in relation to which the Data Users are going to carry out direct marketing. A sample of a consent for direct marketing is shown at **Appendix II**.

5.6.2 If only verbal consent is obtained from a Data Subject, a written confirmation should be issued to the Data Subject within 14 days after the consent is received.

5.6.3 The written confirmation should include:

- date of receipt of the consent;
- permitted types of personal data; and
- permitted class of marketing subjects.

5.7 Valid consent is considered not obtained if a Data Subject refuses to provide his contact information and as a result the written confirmation could not be sent, or when the written confirmation sent to the Data Subject is returned undelivered.

6 Data Security (DPP4)*

Officials should take all practicable steps to safeguard personal data from unauthorized or accidental access, processing, erasure, loss or other uses by adopting the following measures:

6.1 Access control

- Personal data collected and retained should be disseminated to another party only if necessary. Access should be allowed on a "need to know" and "need to use" basis (e.g. when a staff who handles human resources matters is transferred to another post, his right of access to personnel records should cease immediately).
- Measures must be in place to ensure the integrity, prudence and competence of authorized persons (e.g. requiring new staff to read the Code of Practice on Data Protection, requiring staff to participate in data protection refresher workshops periodically, signing of a confidentiality statement by Officials, etc.).
- Personal data should not be taken away from the office, unless under special circumstances (e.g. events that take place outside the office).
- If a Data Processor (e.g. service provider) is engaged, contractual or other means must be adopted to prevent unauthorized or accidental access, processing, erasure, loss or use.

6.2 Data storage

- An appropriate physical location should be identified where the personal data can be safely stored (e.g. lockable filing cabinets or rooms with controlled access or which can be locked when unoccupied). Files containing personal data should not be left open on desks or in areas where they can be seen by unauthorized persons.
- Personal or sensitive data should not be stored in portable devices, such as USB flash drives, notebooks or tablets. In case such data has to be stored in portable / mobile devices temporarily, the data stored should be the minimum necessary and should be password-protected. Moreover, the data must be deleted as soon as the tasks for which it is required have been completed.

6.3 Data transmission

- Officials should adopt appropriate measures to ensure the secure transmission of personal data (e.g. documents containing personal data should be put in a sealed envelope marked "private and confidential" and "to be opened by addressee only" with a specified addressee).
- Officials should make use of shared drives in the computing system if available and, as far as possible, communicate personal information in a safe and restricted environment.
- Personal or sensitive data, when sent electronically, should be password-protected. Email addresses and attachments should be double -checked to ensure that they are correct.
- When sending out a mass email, BCC or mail merge should be used to avoid disclosing the email addresses of recipients.

6.4 Data disposal

- Personal data should be disposed of properly after the specified retention period. For example, hard copy documents should be shredded while disks and memory sticks should be formatted.

6.5 Others

- Information which can lead to the identification of the Data Subject in statistical analysis should be anonymized.

7 Openness (DPP5)

The Federation will make available the following information to all stakeholders:

7.1 Personal data policies and practices adopted;

7.2 Types of personal data held; and

7.3 Purposes for which the personal data is used or to be used.

8 Data Access and Correction (DPP6)

8.1 A Data Subject must be given access to his personal data and allowed to make corrections if it is inaccurate.

8.2 A data access request is a request made by an individual to request the Data User:

8.2.1 to inform him whether the Data User holds personal data of which the individual is the Data Subject; and

8.2.2 if the Data User holds such data, to supply him with a copy of such data.

8.3 Data Subjects are encouraged to make data access requests by means of the form prescribed by the Privacy Commissioner for Personal Data[3].

8.4 Data access requests shall be processed by a DPO who has undergone appropriate training. When the Federation receives a data access request, the DPO should:

8.4.1 ascertain the identity of the requestor; and

8.4.2 assess whether the Federation holds the relevant personal data.

8.5 If the Confederation holds the relevant personal data, a copy of the requested data should be supplied to the Data Subject within 40 calendar days after receiving the request.

8.6 If the Confederation does not hold the requested data, the requestor should still be informed in writing within the 40-day time limit.

8.7 The Confederation shall charge a fee (at $5 per A4-size page) for complying with a data access request.

8.8 The Confederation may refuse to comply with a data access request if:

8.8.1 it is not supplied with sufficient information to identify the requestor;

8.8.2 it cannot comply with the request without disclosing the personal data of a third party; or

8.8.3 where compliance with the request is for the time being prohibited under the Personal Data (Privacy) Ordinance or any other ordinance.

8.9 A log book should be kept to register all data access requests for the past four years, stating reasons if any of them are refused.

9 Opt-out Request*

9.1 In direct marketing, a Data Subject may at any time require a Data User to cease using his personal data. Such "Opt-out" requests may be communicated verbally or in writing.

9.2 To comply with a Data Subject's opt-out request, staff members involved in direct marketing should maintain an "Opt-out List" of all persons who have indicated that they do not wish to receive further marketing approaches.

[3] https://www.pcpd.org.hk/english/publications/files/Dforme.pdf.

10 Handling of Data Breach*

10.1 In case of a data breach, the incident should be reported to the DPO, the respective Office Head, and the Hon Secretary General in the first instance.

10.2 Essential information related to the breach should be gathered.

10.3 The following parties may also be notified as appropriate:

10.3.1 law enforcement agencies;

10.3.2 Office of the Privacy Commissioner for Personal Data; and

10.3.3 IT experts.

10.4 Measures should be adopted to contain the breach (e.g. cessation of a system function or access right).

10.5 An assessment of the potential damage and harm caused by the breach should be made.

10.6 Consideration should be taken to notify affected Data Subjects and relevant parties of the breach. When Data Subjects are not immediately identifiable or where public interest exists, public notification through the Federation's website or media may be considered.

10.7 A thorough investigation into the breach should be carried out. The investigation results should be reported to the Board of Directors and kept in a detailed report.

10.8 Areas for improvement should be identified to prevent the breach from recurring.

10.9 The Data Breach Information Sheet at **Appendix IV** should be used to consolidate information relating to the breach, take remedial actions and conduct post-incident review.

11 Other Relevant Information*

11.1 The Hon Deputy Secretary General of the Confederation shall be the DPO of the Confederation.

11.2 This Code of Practice shall undergo review once every five years.
This version was last updated on 1 April 2021.

Circumstances under which a
Personal Information Collection Statement (PICS) is / is not required

	PICS required:	***PICS <u>not</u> required:***
Event Registration	Personal data is collected directly from participants.	Personal data of corporate team participants is provided by the organization they represent.
Staff Recruitment	Personal data is collected directly from job applicants.	N/A
Membership Programme	Personal data is collected directly from members.	N/A
Lucky draw	Contact details is collected directly from participants.	N/A
Committee Election	Personal data is collected directly from candidates / voters.	Personal data of candidates / voters is provided by NSAs.
Multi-sports Games	N/A	Personal data of delegation members is provided by NSAs.

The list of circumstances outlined above is for reference only and is by no means exhaustive. If in doubt, advice should be sought when deciding if a PICS is required for each individual case.

Appendix II

Sport for All Confederation of Hong Kong, China Limited

Personal Information Collection Statement (Sample)

1. The personal data collected is used by the Confederation for _____ (purpose) or other directly related purpose(s).

2. Please note that it is mandatory for you to provide the personal data marked with asterisks. In the event that you do not provide such personal data, the Confederation may not be able to provide you with _____ (service).

3. Your personal data held by the Confederation will be kept confidential within the retention period, but it may be shared with other parties, including _____ (other organizations), for the purpose(s) stated above.

4. In accordance with the Personal Data (Privacy) Ordinance, you have the right to access, amend, and ask for a copy of your personal data held by the Confederation. Requests for access and/or correction can be made to the Data Protection Officer in writing via email secretariat@sportforallhk.org or by post to Sport for All Confederation of Hong Kong, China Limited, Room 1032A, Olympic House, 1 Stadium Path, Causeway Bay, So Kon Po, Hong Kong. A fee at $5 per A4-size page shall be charged to cover the administrative cost.

5. For further details, please refer to the Confederation's Privacy Policy Statement at link.

Consent for Direct Marketing *(if applicable)*

We intend to use the personal data (name, mobile phone number and email address) you provided in this form for the purpose of sending you information about activities organized by us. We cannot use your personal data unless we have received your consent or indication of no objection.

If you do not agree to such use, please indicate your objection by ticking the box below:

☐ I do not wish my personal data to be used for the above-mentioned purpose(s).

_____

Name and signature

Date:

Appendix III

Sport for All Confederation of Hong Kong, China Limited

Personal Data Inventory (Sample)

Office / Division:	Admin Division	Secretariat
Category of record	Personnel records	Voters register for the Athletes Committee Election
Items of personal data contained in the record	- Name - Contact information (including address, mobile phone number and email address) - Bank account details - MPF scheme registration - Remuneration package - Leave records - Academic qualifications	- Name - Gender - Email address - Affiliated NSA - Asian Games Accreditation Card No. (collected from online registration forms only) - Participation record in the last three editions of the Asian Games or other Multi-Sports Games.
Means of collection of the data	Employee Information Form	Information provided by NSAs, Voter Registration Forms received by email or filled online
Purpose of collection and use of the data	Handle employment-related matters	Handle matters related to the Confederation Committee Election
Retention period of the data	7 years after the employee has left the service	4 years after the voter is no longer eligible to vote
Location for data storage	Physical: filing cabinets of the Secretariat Electronic: computers of the Secretariat	Electronic: network drive of Admin Division

Disclosure of data to any third parties including Data Processors (e.g. service providers) and the names and relevant details of third parties (Yes/No)	No	- Some data (name, email address, affiliated NSA, and Asian Games Accreditation Card No.) were collected via Google Forms. - Some data (name, email address only) were transferred to Election Runner to enable online voting.
Possible location of transfer (e.g. cloud server location)	N/A	Network drive of Google Forms / Election Runner
Purpose of disclosing the data and whether the disclosure complies with the Personal Data (Privacy) Ordinance (Cap 486)	N/A	Enable online submission of Voter Registration Form and online voting (Data Subjects were aware of / informed about this)
Date of return or destruction by the Data Processor (if applicable)	N/A	1 year after the completion of the election
Security measures adopted	Filing cabinets are locked and the key is kept by Hon. Deputy Secretary General	- The Secretariat's network drive can only be accessed by designated staff of the Secretariat.

Appendix IV

Sport for All Confederation of Hong Kong, China Limited

Data Breach Information Sheet

Office / Division:	
A) Information of the Breach	
(i) General information of the breach	
Description of the breach	
Date and time of the breach	
Location of the breach (e.g. which office, which computer server, etc.)	
Date and time of discovering the breach	
How the breach is discovered (e.g. discovered during routine system checking, known after reported by media, etc.)	
Nature of the breach (e.g. loss of data, database is hacked, etc.)	
Cause of the breach	
(ii) Impact of the breach	
Types of Data Subjects affected (e.g. staff, members, public, etc.)	
Estimated number of Data Subjects affected (Please state the respective number for each type of Data Subjects)	
Types of personal data affected (e.g. name, date of birth, HKID card number, address, telephone number, etc.)	
Medium holding the affected personal data (e.g. physical folders, USB, etc.)	
If the personal data is held in electronic medium, is the data encrypted?	
B) Data Breach Notification to Regulatory Bodies	
Are other regulatory bodies such as the Hong Kong Police Force or the Office of the Privacy Commissioner for Personal Data, Hong Kong being notified of the breach? If yes, please provide the date and details of each notification given.	

C) Actions Taken / To be Taken to Contain the Breach	
Brief description of actions taken to contain the breach	
Please evaluate the effectiveness of the abovementioned actions taken	
Brief description of actions that will be taken to contain the Breach	
D) Risk of Harm	
Please assess the potential harm to Data Subjects caused by the breach and the extent of it	
E) Data Breach Notifications to Data Subjects Affected	
Dates and details of the data breach notifications issued to data subjects affected by the breach	
If no data breach notification is issued/will be issued, please state the consideration	
F) Investigation Results	
Cause(s) of the breach	
G) Post-incident Review (To be completed by the Data Protection Officer)	
Recommended improvement measures and the respective implementation date	
Date to review the effectiveness of the abovementioned improvement measures	

Completed by
(Office Head)

Signature: _____

Name: _____

Post _____

Date: _____

Reviewed by
(Data Protection Officer)

Signature: _____

Name: _____

Post _____

Date: _____